UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/541,697	04/18/2006	Marian Trinkel	20811/0204765-US0	1949

95402 7590 07/20/2010

LEYDIG, VOIT AND MAYER
TWO PRUDENTIAL PLAZA, SUITE 4900
180 NORTH STETSON AVENUE
CHICAGO, IL 60601

EXAMINER	
ARMOUCHE, HADI S	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
07/20/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/541,697	TRINKEL, MARIAN	
	Examiner	Art Unit	
	HADI ARMOUCHE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 June 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-10 and 12-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-10 and 12-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 06/09/2010 has been entered.

2. Claims 1, 4, 9 and 18-20 have been amended; claims 3 and 11 have been cancelled. Claims 1-2, 4-10 and 12-20 remain pending.

Response to Arguments

3. Acknowledgment to applicant's amendment to the specification has been noted. The specification has been reviewed, entered and found obviating to previously raised objection to the specification for minor informalities. Objection to the specification is hereby withdrawn.

4. Acknowledgment to applicant's amendment to claims 19 and 20 has been noted. The claims has been reviewed, entered and found obviating to previously raised objection for minor informalities. Objection to claims 19 and 20 is hereby withdrawn.

5. Applicant's arguments filed on 06/09/2010 have been fully considered but they are not persuasive.

6. It has been argued (pages 10 and 11 of the remarks) that the combined teachings of Hartman, Fruehauf, and Sinha fail to disclose or suggests that *the central*

system comprising a plurality of clock systems and plurality of network users each comprising a clock system, wherein each of the plurality of clock systems of the central system is uniquely assigned to one of the plurality of network users for synchronously create a key for the network user.

7. Applicant's interpretation of the references is noted. However examiner respectfully disagrees. The rejection was structured so that the three references (Hartman, Fruehauf and Sinha) would be taken in combination. Sinha teaches that *the central system comprising a plurality of clock systems* [col 3 lines 17-22 and col 5 lines 51-56]

and plurality of network users each comprising a clock system [Figure 1 elements 124, 126, 128, col 5 lines 51-56 and col 10 lines 1-3]

wherein each of the plurality of clock systems of the central system is uniquely assigned to one of the plurality of network users [col 5 lines 51-56, col 12 lines 61-62 and col 17 line 58-col 18 line 13]

col 3 lines 17-22

> Embodiments of the present invention include methods, systems and apparatus for synchronizing a slave first clock to a master first clock. Information from the master about a timing relationship between the master first clock and a master second clock may be used to synchronize a slave second clock to the master second clock.

col 5 lines 51-56

> The ensuing description refers to master clocks on one side of a communication link, and slave clocks on the other side, with each slave being adjusted to match the master. A plurality of such clock master-slave pairs may exist across a given

link, and in one aspect the interrelationship between at least two such pairs is described.

col 10 lines 1-3

Those skilled in the art will have no difficulty extending the synchronization to a multiplicity of CPEs linked to a base station 300, as are described above.

col 12 lines 61-62:

It is preferred that the slave symbol clock be phase-locked to the master symbol clock.

col 17 line 58-col 18 line 13

The network clock will generally not be available for explicit communication across the link, because such explicit communication generally requires too much of the available communication media, whether optical, wired or RF wireless. Moreover, the network clock will in general be entirely asynchronous to the (e.g.) symbol clock. The symbol clock (or any such clock separate from the network clock) is independently synchronized across the link, as described in the previous sections. It may be unnecessary to phase lock the network clock, since in many instances a frequency lock will suffice. If a first independent pair of clocks is synchronized across the link, as described above, then one may efficiently synchronize a second, independent pair of clocks across the same link by conveying data to the slave side which reflects a relationship on the master side between the first (synchronized) clock and the second independent clock. Thus, the synchronized symbol clocks described above may provide part of a solution for synchronizing constant bit-rate (CBR) data transfers across a communication link. Synchronized clocks, such as those described, may serve as "noncommon clocks" which may be leveraged to synchronize other independent clocks across the same link.

Sinha in figure 1 simply shows that one of the master clocks (CNET A) is uniquely assigned to one of the plurality of network users' (user 124) clock (CNET D). Nowhere in Sinha does he teach that the CNET D clock is common among all the other users (users 126 and 128) as applicant argues. Sinha as cited above teaches that each slave

has its own clock that corresponds to a master clock. Sinha to simplify his illustration, shows how one slave will synchronize with the master.

Whereas Fruehauf teaches *synchronously creating the key by the clock system of the central system and a clock system of the network user uniquely assigned to the network user* [Figure 1 elements 103, 116; col 2 lines 14-34; col 4, line 65-col 5 line 16].

col 4, line 65-col 5 line 16:

> Referring back to FIG. 1, the data encryptor 107 and the data decryptors 112-114 obtain a key from the key storage units 104 and 117, respectively, which generate keys based on the time data in clocks 103 and 116 ("key time"). After initially obtaining a key, periodic key changes are performed by the data encryptor 107 and the data decryptors 112-114 by obtaining a new key from the key storage units 104 and 117, respectively. The key storage units 104 and 117 assign a new key to the data encryptor 107 and the data decryptors 112-114, respectively, at each key time according to the clocks 103 and 116, respectively. The data encryptor 107 and the data decryptors 112-114 hold the same key until another key time occurs ("key period") according to the clocks 103 and 116, respectively. The length of the key period is variable and is preferably a function of the user's security level requirements and the long-term accuracy of the clocks 103 and 116. The length of the key period may be set at a range from several days to nanoseconds if the timing mechanisms in the system are sufficiently accurate to maintain sychronization.

Claim Rejections - 35 USC § 103

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. Claims 1-2, 9-10, 15-17 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman Jr. (5,444,780), hereafter referred to as Hartman, in view of

Fruehauf et al. (US 6,590,981), hereafter referred to as Fruehauf, and further in view of Sinha et al. (US 6,944,188), hereafter referred to as Sinha.

Regarding claim 1:

Hartman teaches *a method for receiving a request from one of a plurality of network users for a time signal* [col 4 lines 64-68];

encrypting said time signal with at least one key [col 4 lines 54-56 and col 5 lines 28-35];

transmitting the encrypted time signal to the one of the plurality of network user via a telecommunications network [col 5 lines 35-37];

Hartman fails to explicitly disclose *synchronously creating the key by the clock system of the central system and a clock system of the network user uniquely assigned to the network user.*

Fruehauf teaches *synchronously creating the key by the clock system of the central system and a clock system of the network user uniquely assigned to the network user* [Figure 1 elements 103, 116; col 2 lines 14-34; col 4, lines 65-col 5 line 16].

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Hartman to synchronously create symmetric keys, as taught in Fruehauf. The motivation/suggestion would have been to prevent the loss or rejection of valid data.

The combined teachings of Hartman and Fruehauf fail to disclose that *the central system comprising a plurality of clock systems, wherein each of the*

plurality of clock systems of the central system is uniquely assigned to one of the plurality of network users; identifying, by the central system, one of the plurality of clock systems thereof uniquely assigned to the network user.

Sinha teaches that *the central system comprising a plurality of clock systems* [col 3 lines 17-22 and col 5 lines 51-56]*, wherein each of the plurality of clock systems of the central system is uniquely assigned to one of the plurality of network users* [col 5 lines 51-56, col 9 line 59-col 10 line 3, col 12 lines 61-62 and col 17 line 58-col 18 line 13]*; identifying, by the central system, one of the plurality of clock systems thereof uniquely assigned to the network user* [col 5 lines 51-60 and col 12 lines 61-62].

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the combined teachings of Hartman and Fruehauf to allow clocks to be paired in master and slave pairs, as taught by Sinha. The motivation/suggestion would have been to match the rate at which data is received.

Claim 9 has same limitations as claim 1 and hence same rejection rational is applied. Additional limitation include *wherein the network user is configured to decrypt the encrypted time signal* [Hartman, col 5 lines 38-43].

Regarding claims 2 and 19: A system that dynamically changes symmetric keys after a predetermined period of time can be seen in **Fruehauf column 2, lines 7-10, 14-34**, which discloses a cryptographic communication system with time synchronized keys that change after a predetermined period of

time, being used for encryption and decryption between sender and receiver locations.

Regarding claim 10: A system in which the central system includes a time signal transmitter can be seen in **Sinha column 3, lines 5-11; column 7, line 61 to column 8, line 3; Fig. 3**, which discloses a system that uses a transmitter as part of the master clock.

Regarding claim 15: A system in which a user decrypts an encrypted time signal can be seen in **Hartman column 5, lines 38-43**, which discloses a system where the client decrypts the encrypted time signal that it received from a secure time server.

Regarding claims 16, 17, and 20: A system in which the central system is a certified central system can be seen in **Fruehauf column 3, line 47 to column 4, line 15**, which discloses a system that uses officially recognized time sources to create a time signal.

10. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman in view of Fruehauf, and Sinha, and in further in view of Crane et al. (US 6,510,236), hereafter referred to as Crane.

Regarding claim 4: The combined teachings of Hartman, Fruehauf, and Sinha fail to explicitly disclose a system that determines, by the central system, a clock system assigned to the network user using a transmitted identifier, wherein the transmitted identifier is the network address of the network user.

However, **Crane column 4, line 48 to column 5, line 36** discloses a system in which a device-id is used to locate the corresponding server.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the combined teachings of Hartman, Fruehauf, and Sinha to use a device's corresponding id, as taught by Crane, as the device's id is known by both parties and can easily be used to create corresponding symmetric keys.

11. Claims 5-8 and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman in view of Fruehauf and Sinha, and further in view of Kara (US 5,982,506), hereafter referred to as Kara.

Regarding claim 5: Hartman and Fruehauf fail to explicitly disclose a system that transmits the time signal and the data from the first network user to the second network user using one of directly and indirectly via the central system.

However, **Kara column 19, lines 19-31** discloses a system in which a sender and a receiver communicate directly with one another without the intervention of a central system.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow the sender and receiver to communicate with each other without relying on a central system, as taught in Kara, to hasten transaction speed between the two devices.

Kara column 4, lines 25-56 discloses an invention that sends a message from a sender to a receiver via a certification system.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to send a message indirectly through a central system, as taught by Kara, so that the send time may be verified and certified by an external third party.

Regarding claim 6: A system in which the first network user encrypts at least one of the data and the time signal during transmission can be seen in **Kara column 4, lines 43-48; column 7, lines 43-45**, in which the electronic document and/or the cipher containing the timestamp may be encrypted.

Regarding claims 7 and 12: A system in which the central system can be provided at the second network user can be seen in **Kara column 25, lines 47-61**, in which the certification and key distribution authority can be located at the receiving location.

Regarding claims 8, 13 and 14: A system in which the central system returns an acknowledgment to the network user can be seen in **Kara column 4, line 65 to column 5, line 22**, in which the receiver sends an acknowledgement message to the certification program which forwards the acknowledgement to the sender upon successful verification.

12. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman in view of Fruehauf, Sinha and Crane, and further in view of Friedman et al. (US 2002/0019933), hereafter referred to as Friedman.

Regarding claim 18: Hartman, Fruehauf, Sinha, and Crane fail to explicitly disclose that the key is created using at least one of the assigned clock based on the transmitted identifier.

However, **Friedman [0101]** discloses a system in which a key is derived using information unique to the particular requesting device.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to use a device's corresponding id, as taught by Friedman, as the device's id is known by both parties and can easily be used to create corresponding symmetric keys.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HADI ARMOUCHE whose telephone number is (571)270-3618. The examiner can normally be reached on M-Th 7:30-5:00 and Fridays half day.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H. A./
HADI ARMOUCHE
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432